Einführung in die Kryptographie: Methoden und praktische Anwendungen

Praxisnahe Übersicht: Methoden und Anwendungen der Kryptographie

Beginn:
29.04.2027 - 09:00 Uhr

Ende:
30.04.2027 - 16:30 Uhr

Dauer:
2,0 Tage

Ostfildern

Veranstaltungsnr.: **36257.00.004**

Leitung

Dr. Julian Liedtke
TRUMPF SE + Co. KG

Alle Referent:innen

Präsenz
EUR 1.310,00
(MwSt.-frei)

Mitgliederpreis
EUR 1.179,00
(MwSt.-frei)

in Zusammenarbeit mit:

GESELLSCHAFT FÜR INFORMATIK



BESCHREIBUNG

[redacted]

BESTE ANBIETER WEITERBILDUNG 2026/27 stern

FOCUS TOP ANBIETER FÜR WEITERBILDUNG 2026 Technische Akademie Esslingen e. V. FOCUS.DE/BUSINESS



Security in Produkten stützt sich insbesondere in der Umsetzung technischer Anforderungen. Fehler, falsche Entscheidungen, unzureichende Kenntnisse öffnen potenziellen Angreifern Möglichkeiten (und seien sie noch so klein) Sicherheitsziele zu kompromittieren und Werte zu verletzen/zerstören. In diesem Kurs werden praxisnah die Methoden der Kryptographie vorgestellt und deren Vor- und Nachteile evaluiert.

Ziel der Weiterbildung

- Überblick über Methoden und Algorithmen der Kryptographie kennenlernen
- Bewusstsein bekommen, wann welche Methoden eingesetzt werden
- Hilfen zur Bewertung von Kryptographie kennen
- Anwendungsfälle exemplarisch kennenlernen
- Unterschiede von funktionaler Sicherheit und Security kennen
- Risikobegriff kennen
- Vor- und Nachteile der einzelnen Methoden nach Anwendung beurteilen (z.B. Integrität versus Vertraulichkeit)
- geeignete Methoden zur Umsetzung von Regularien wie z.B. Produktsicherheit nach dem Cyber Resilience Act (CRA) kennen und einsetzen können

PROGRAMM

Donnerstag, 29. und Freitag, 30. April 2027
9:00 Uhr bis 16:30 Uhr, inkl. Pausen

1 | Intro und Motivation

- Motivation, Anwendungsfälle
- CIA-Triade
- Beispiele für Angriffe (Ransomware, Vishing, CEO-Fraud, KRACK, ...)
- Safety vs. Cybersecurity
- BSI
- STRIDE-Bedrohungsmodellierung
- Historie der Kryptographie
- Steganographie
- Kerkhoff's Prinzip

2 | Landkarte

- Landkarte der Kryptographie

3 | Symmetrische Verschlüsselung

- Grundbausteine: Substitution und Transposition
- Kryptoanalyse
- Man-in-the-middle
- Häufigkeitsanalyse
- Brute Force Attack
- Lineare Kryptoanalyse
- Substitutions-Permutations-Netzwerke (SPNs)
- Block Ciphers
- Block Cipher Modes (ECB, CBC, CTR)
- Advanced Encryption Standard (AES)
- Padding und Padding Angriffe
- Vernam-Verschlüsselung, One-Time-Pad (OTP)
- Chosen-Plaintext Attack (CPA)
- Chosen-Ciphertext Attack (CCA)
- Stream Ciphers (Enigma)
- Pseudo-Random Functions (PRF)
- Roll Jam Technique
- Auswahl eines für den Use-Case passenden Verfahrens
- Vor- und Nachteile, Einordnung und mögliche Alternativen

4 | Hash Funktionen & Message Authentication Codes (MACs)

- Anwendungsfeld und Einsatzmöglichkeiten (Digitale Signaturen, Public Key Encryption, Message Authentication Codes, ...)
- Auswahl eines für den Use-Case passenden Verfahrens
- Vor- und Nachteile, Einordnung und mögliche Alternativen
- Gegensatz zu Cyclic Redundancy Checks
- Hamming Distanz
- Preimage Resistance
- Collision Resistance
- Message Authentication Codes mittels Hashes (Encrypt-then-MAC)
- Geburtstagsparadoxon
- Einwegfunktionen
- Kompressionsfunktion
- Sponge-Funktionen
- Password Security
- Authentication
- Rainbow Tabellen
- Salt und Pepper
- Multi-Faktor-Authentifizierung
- Time-based One-time Passwort (TOTP)

5 | Message Authentication Codes (MACs)

- Secret-Prefix
- Secret-Suffix
- HMAC (Hash-based Message Authentication Code)
- CMAC (Cipher-based Message Authentication Code)
- Forgery-Sicherheitseigenschaft
- Hashing mit Schlüssel
- Replay Attacke

6 | Authenticated Encryption

- Encrypt-and-MAC
- MAC-then-Encrypt
- Encrypt-then-MAC

7 | Asymmetrische Verschlüsselung

- Anwendungsfeld und Einsatzmöglichkeiten
- Modulo-Operation
- zahlentheoretische, schwierige Probleme
- RSA-Verschlüsselung
- OAEP: Optimal Asymmetric Encryption Padding
- Diffie Hellmann (DH) Key Exchange

8 | Digitale Signaturen

- Digitale Signaturen
- Public Key Infrastructure (PKI)
- Certificate Authorities (CAs)
- Chain of trust
- Certificate Revocation Liste (CRL)
- Online Certificate Status Protocol (OCSP)
- Relay Station Attack (RSA)

9 | Weiterführende Themen

- Post-Quantum Kryptografie: Learning with Errors (LWE)
- Quanten Computer
- Shor Algorithmus
- Zero-knowledge Proofs

10 | Summary

- Auswahl eines für den Use-Case passenden Kryptosystemes
- Vor- und Nachteile, Einordnung und mögliche Alternativen

REFERENT:INNEN

Dr. Julian Liedtke
TRUMPF SE + Co. KG

Dr. Julian Liedtke ist Experte für Cybersicherheit mit Schwerpunkt auf Cyber Resilience Act und Network and Information Security (NIS-2, ISO 27001). Als Cyber Security Coordinator verantwortet er die Umsetzung und Einhaltung wichtiger Sicherheitsregulierungen. Seine Aufgaben umfassen die Koordination von Sicherheitsmaßnahmen und die Entwicklung von Strategien zur Cyberresilienz. Im Jahr 2024 schloss er seine Promotion in Informatik ab, was seine akademische Expertise unterstreicht. Seine Kombination aus wissenschaftlicher Ausbildung und praktischer Erfahrung macht ihn zu einem gefragten Spezialisten. Dr. Liedtke

trägt maßgeblich zur Weiterentwicklung von Sicherheitskonzepten in der digitalen Infrastruktur bei.

Dr. Thomas Liedtke

Dr. Thomas Liedtke ist
- seit vielen Jahren beratend tätig für funktionale Sicherheit, Informations- und Produktsecurity. Er ist Mitglied der deutschen DIN-AK-Spiegelgruppe, welche für die Definition ISO/SAE 21434, ISO/PAS 5112 und weitere Cybersecuritystandards verantwortlich ist
- Mitglied des intacs Advisory Boards und Leiter der SPICE Cybersecurity Arbeitsgruppe Leiter der ZVEI Arbeitsgruppe Datensicherheit im Automobil
- Leadauditor für CSMS; ISMS; TISAX
- Berater für die Implementierung der Cybersecurity in Unternehmen Publikationen
- Informationssicherheit: Möglichkeiten und Grenzen; SpringerLink publisher: link.springer.com/book/10.1007/978-3-662-63917-7
- The New Cybersecurity Challenges and Demands for Automotive Organisations and Projects – an Insight View link.springer.com/chapter/10.1007/978-3-031-42307-9_21

Weitere Veranstaltungen

Cyber Resilience Act (CRA) – Anforderungen und Pflichten für Unternehmen

NIS-2-Richtlinie im Gesundheitswesen rechtskonform umsetzen

Cyber Resilience Act (CRA) in der Produktentwicklung

Sicherheitsgerichtete Systeme entwickeln

VERANSTALTUNGSORT UND HOTEL

Technische Akademie Esslingen
An der Akademie 5
73760 Ostfildern



Anfahrt
Die TAE befindet sich im Südwesten Deutschlands im Bundesland Baden-Württemberg – in unmittelbarer Nähe zur Landeshauptstadt Stuttgart. Unser Schulungszentrum verfügt über eine hervorragende Anbindung und ist mit allen Verkehrsmitteln gut und schnell zu erreichen.

Hotelübernachtung benötigt?

Über den nachfolgenden Link finden Sie nahegelegene Hotels in direkter Umgebung zu TAE-Konditionen:

Hotelbuchung

GEBÜHREN UND FÖRDERMÖGLICHKEITEN

Die Teilnahme beinhaltet Verpflegung sowie ausführliche Unterlagen.

Preis:
Die Teilnahmegebühr beträgt:

1.310,00 € (MwSt.-frei)

Fördermöglichkeiten:
Für den aktuellen Veranstaltungstermin steht Ihnen die ESF-Fachkursförderung leider nicht zur Verfügung.

Für alle weiteren Termine erkundigen Sie sich bitte vorab bei unserer Anmeldung.

Andere Bundesland-spezifische Fördermöglichkeiten finden Sie hier.

Inhouse Durchführung:
Sie möchten diese Veranstaltung firmenintern bei Ihnen vor Ort durchführen? Dann fragen Sie jetzt ein individuelles Inhouse-Training an.

IMMER TOP!

Unser Qualitätsversprechen



Seit über 65 Jahren gehört die Technische Akademie Esslingen (TAE) mit Sitz in Ostfildern – nahe der Landeshauptstadt Stuttgart – zu Deutschlands größten Weiterbildungs-Anbietern für berufliche und berufsvorbereitende Qualifizierung im technischen Umfeld. Unser Ziel ist Ihr Erfolg. Egal ob Seminar, Zertifikatslehrgang oder Fachtagung, unsere Veranstaltungen sind stets abgestimmt auf die Bedürfnisse von Ingenieuren sowie Fach- und Führungskräften aus technisch geprägten Unternehmen. Dabei können Sie sich stets zu 100 Prozent auf die Qualität unserer Angebote verlassen. Warum das so ist?